REMARKS

Claim 18 has been amended. Claims 33-36 have been added. Hence, Claims 1, 2, 4, 8-10, 13-20 and 23-36 are pending in the application. The amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to exclusively improve readability and clarity of the claims and not for the purpose of overcoming alleged prior art.

Each issue raised in the Office Action mailed April 10, 2006 is addressed hereinafter.

I. ISSUES NOT RELATING TO CITED ART

Claims 1, 8, 18 and 30-32 stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The rejection is respectfully traversed.

The Office Action asserts that the terms "longer-lived symmetric key" and "shorter-lived symmetric key" in independent claims 1, 8, 18, and 30-32 are relative terms which render the claims indefinite. However, according to MPEP, "[t]he fact that claim language, including terms of degree, may not be precise, does not automatically render the claim indefinite under 35 U.S.C. 112, second paragraph" (2173.05(b)).

In Applicant's Application, it is clearly specified that any appropriate lifetime or term may be selected for the Device Symmetric Key (i.e., longer-lived symmetric key) and for the Short-Term Device Symmetric Key (i.e., shorter-lived symmetric key) (paragraph 0097).

The Specification clearly specifies that the longer-lived symmetric key is established in a key registration phase (paragraph 0070). While a device may carry out the key registration phase any number of times, but in practice it is expected that the device will carry out the key

registration phase only periodically over a relatively long time interval, e.g., once upon booting up or initiating operation, once a day, etc. (*Id.*).

On the other hand, the shorter-lived symmetric key is used for specific tasks such as authentication, key agreement, etc. for the lifetime of the short-lived key, as determined by a policy associated with the shorter-lived key (Specification, paragraph 0092).

In one embodiment, the shorter-lived symmetric key is shorter than that of the longer-lived symmetric key (Specification, paragraph 0097).

In light of the disclosure in the Specification, one of ordinary skill in the art will understand what is claimed by the independent claims 1, 8, 18, and 30-32. Therefore, it is respectfully submitted that Claims 1, 8, 18, and 30-32 are definite under 35 U.S.C. § 112, second paragraph. Applicant requests reconsideration of the rejections under 35 U.S.C. § 112, second paragraph.

II. ISSUES RELATING TO CITED ART—DAVID IN VIEW OF LOTSPIECH

Claims 1, 8, 18 and 30-32 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Davis WO 99/17495 (*Davis*) in view of Lotspiech et al., U.S. Patent Publication No. 2002/0147906 A1 (*Lotspiech*) and Bruce Schneier 1996 (*Schneier*). The rejection is respectfully traversed.

As best as Applicant can determine, the Office Action only correlates Claim 18 with passages in the cited art. The Office Action does not provide a specific identification of which passage(s) in the cited references allegedly correlates to each feature of the rest of independent claims 1, 8, and 30-32. Therefore, the Office Action has failed to establish a prima facie case that those independent claims 1, 8, and 30-32 are unpatentable over the cited art. Furthermore, to an extent, Applicant has had to engage in guesswork in making up the missing correlation between the claims and the references cited in the Office Action. Clarification is requested.

A. Claim 1.

As amended, independent Claim 1 features the following:

providing, using a secure communication channel, information identifying a trusted device registration service to a first non-configured network packet-routing device for use in obtaining a longer-lived symmetric key;

providing trusted information to the trusted device registration service that certifies that the first device is a known device within a security realm;

authenticating the first device to the trusted device registration service;

registering the first device in the network at the trusted device registration service, wherein the trusted device registration service establishes a longer-lived symmetric key and provides the first device with the longer-lived symmetric key; ...

The cited references fail to teach, disclose or suggest all the features of Claim 1.

1. Providing Information Identifying a Trusted Device Registration Service and Using a Secure Communication Channel

The proposed combination of *Davis, Lotspiech* and *Schneier* does not provide the features of providing information identifying a trusted device registration service as recited in Claim 1. Likewise, the proposed combination does not provide the features of using a secure communication channel as recited in Claim 1.

The Office Action implies that a passage of *Davis* (page 7 lines 10-15) as disclosing the aforementioned features. However, *Davis* makes no mention of a feature of information identifying a trusted device registration service, much less a feature of providing the same.

Davis also fails to disclose using a secure communication channel for the purpose of registration or receiving keys. For example, *Davis* specifically teaches away from a secure communication channel, stating that the "registration scheme does not require a secure communication channel" and a communication channel between the electronic system and the

database "may be accomplished over the Internet, through a dedicated phone line or **over any other communication link**" (*Davis* page 8 the last line – page 7 the first line) (emphasis added).

2. Security Realm

The proposed combination of *Davis, Lotspiech* and *Schneier* does not provide the feature of a security realm as recited in Claim 1.

The Office Action implies that a passage of *Davis* (page 7 lines 10-15) as disclosing this feature. However, *Davis* makes no mention of a feature of a security realm in the cited passage or anywhere in the reference.

3. Establish a Longer-Lived Symmetric Key at the Time of Registration

The proposed combination of *Davis, Lotspiech* and *Schneier* does not provide the feature of establishing a longer-lived symmetric key as recited in Claim 1.

The Office Action implies that a combination of *Davis* and *Lotspiech* (paragraphs 0014 and 0046) discloses this feature. However, even assuming *Lotspiech*'s long-lived and short-lived keys were incorporated into *Davis*'s device, the combination would still be different with respect to the aforementioned feature of Claim 1.

First, the longer-lived key in Claim 1 is established at the time of registering the device at a registration service, not at the time of manufacturing the device as in *Davis*. Since a device is manufactured only once, the key as disclosed in *Davis* or in the suggested combination would only be generated once. In Claim 1, however, the longer-lived symmetric key (and different values thereof) can be established again and again after the device is manufactured. For example, a new longer-lived symmetric key can be established in a new key registration phase in a new booting process or when the device is installed in a new location and re-registered.

4. Authenticating the Longer-Lived Symmetric Key

The proposed combination of *Davis, Lotspiech* and *Schneier* does not provide the feature of generating and providing a shorter-lived symmetric key to the first device based on **authenticating the longer-lived symmetric key** as recited in Claim 1.

The Office Action admits that *Davis* fails to disclose this feature. Furthermore, neither *Lotspiech* nor the proposed combination of *Davis* and *Lotspiech* (paragraphs 0014 and 0046) could possibly disclose this authentication feature with respect to the longer key that is provisioned to the device by the registration service. In *Davis*, for example, once a PRK (which is analogous to the longer-lived symmetric key of Claim 1 according to the Office Action) is sent to the device, the PRK is not received again and *Davis* does not describe authenticating the device on the basis of verifying the PRK. Thus, even if, in the proposed combination, *Davis*'s PRK is substituted by a longer-lived symmetric key in *Lotspiech,* the feature of authentication with respect to the longer-lived symmetric key is still missing from such a combination, because *Lotspiech* does not even mention such an authentication feature.

5. Receiving a Request from a Second Device

The proposed combination of *Davis, Lotspiech* and *Schneier* does not provide the feature of receiving a request from a second network packet routing device to obtain a session key as recited in Claim 1.

The Office Action admits that *Davis* and *Lotspiech* fail to disclose this feature. Moreover, contrary to the assertion made in the Office Action, *Schneier* also does not disclose the aforementioned features. Fig. 24.1, which the Office Action alleges as disclosing this feature, does not show any second device, let alone a second device that, on behalf of itself and a first device, sends a request for a session key in response to a request from the first device, as recited in Claim 1.

Furthermore, since *Davis* and *Lotspiech* does not disclose any second network packet routing device, neither reference can possibly offer any motivation and suggestion for a combination that comprises a second network packet routing device.

For the reasons set forth above, since neither *Davis* nor *Lotspiech* nor *Schneier* teaches or suggests each and every feature of Claim 1, it is respectfully submitted that Claim 1 is patentable under 35 U.S.C. 103(a) over the cited references.

B. Claims 8 and 30-32

Claims 8 and 30-32 recite similar features to those already discussed with respect to Claim 1. For example, each of Claims 8 and 30-32 at least recites the features of a secure communication channel, information identifying a registration service, establishing a longer-lived symmetric key, authenticating a device based on a longer-lived symmetric key, receiving a request from a second device for a session key, etc. Thus, for at least the similar reasons set forth before, each of Claims 8 and 30-32 is patentable under 35 U.S.C. 103(a) over the cited references.

C. Claim 18

Claim 18 recites similar features to those already discussed with respect to Claim 1. For example, Claim 18 at least recites the features of a secure communication channel, information identifying a registration service, authentication based on a longer-lived symmetric key, a request from a second device for a session key, etc. Thus, for at least the similar reasons set forth before, Claim 18 is patentable under 35 U.S.C. 103(a) over the cited references.

III. ISSUES RELATING TO CITED ART--SPRUNK IN VIEW OF GANESAN AND DAVIS

Claims 1-5, 8-10, 12-20 and 23-32 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Pat. App. Pub. No. 2005/0027985 A1 to Sprunk et al.

(*Sprunk*) in view of U.S. Pat. No. 5,737,419 to Ganesan (*Ganesan*), and *Davis*. The rejection is respectfully traversed.

A. Claim 1.

The cited references fail to teach, disclose or suggest all the features of Claim 1.

1. The Cited References Do Not Teach A Method For Registering A Non-Configured Device.

The Office Action admits *Sprunk* and *Ganesan* do not teach configuring a non-configured network device. But the Office Action asserts that *Davis* discloses configuring a non-configured network device. Applicant respectfully disagrees.

Configuring a cryptographic device in *Davis* is not analogous to configuring a non-configured network device. In fact, the configuration phase in *Davis* "involves loading a device serial number (DSER) and a symmetric key (SK) into non-volatile memory (215) of the cryptographic device (150)" (Abstract). The cryptographic device (15) is then installed to an electronic system that is subsequently released to a downstream customer (*Davis* page 8 lines 10-13; lines 15-17) and, presumably, would then be connected to a network. Clearly, configuring the cryptographic device, which is an internal component of a networked device as the electronic system, occurs when the electronic system in *Davis* is manufactured. Therefore, when the cryptographic device (15) is installed into the electronic system, the configuration phase for the cryptographic device is already over. The only step left in *Davis* is registration.

However, the *Davis* registration only involves recovering some information that was previously configured at the manufacturing time. Thus, the registration process of the electronic system in *Davis* does not involve configuring an unconfigured network device as claimed in Claim 1. For example, Claim 1 recites, but *Davis* fails to disclose, establishing a longer-lived symmetric key at the time of configuring the unconfigured network device. In fact, *Davis* does not establish any longer-lived symmetric key because all the keys (PUK/PRK) have been

previously configured at the manufacturing time with respect to the cryptographic device, and PUK/PRK is a pair of asymmetric keys.

Since none of the cited references discloses or teaches configuring an unconfigured network device, it is respectfully submitted that the cited references fails to teach a method as recited in Claim 1.

2. The Cited References Do Not Teach a Longer-lived Symmetric Key.

In Claim 1, a longer-lived symmetric key is established and provided to a first device. The first device can request a shorter-lived symmetric key using a message containing the longer-lived symmetric key. The longer-lived symmetric key in the message is used to authenticate the first device. If the authentication is successful, a shorter-lived symmetric key is provided to the first device. The use of the shorter-lived symmetric key has an effect of limiting the amount of time that the longer-lived symmetric key may be compromised.

None of these features relating to the longer-lived symmetric key is disclosed in *Sprunk*, *Ganesan*, or *Davis*. *Sprunk* discloses a manufacturer generated lifetime certificate (CTA certificate) (paragraph 105). But, just like the PRK/PUK in *Davis* previously discussed, the CTA certificate is distinguishable from a longer-lived symmetric key claimed in Claim 1 in that CTA certificate is placed in CTA at the time of CTA being manufactured (*Id.*). As noted before, similar to DSER and SK in *Davis,* since the device would presumably be manufactured only once, the CTA certificate as disclosed in *Sprunk* or in the suggested combination would only be generated once. On the other hand, in Claim 1 the longer-lived symmetric key is established each time a key registration phase occurs.

Likewise, a SC Ticket (320 of Fig. 3) in *Sprunk* is different from the longer-lived symmetric key in that the SC Ticket is used by CTA to access a signaling controller's service.

But, in Claim 1, the longer-lived symmetric key is sent back to the trusted device registration service to obtain a shorter-lived symmetric key from a as claimed in Claim 1.

Finally, neither *Ganesan* nor *Davis* discloses the features relating to a longer-lived symmetric key as claimed in Claim 1.

3. The Cited References Do Not Teach Receiving a Request from a Second Device to Obtain a Session Key on Behalf of Both the First Device and the Second Device.

Claim 1 features a second device sending a request for the session key on behalf of both the first device and the second device.

Sprunk does not teach or suggest receiving a request from a second device to obtain session keys ***on behalf of both*** a first device and the second device. Although the KDC receives requests from each device for a session key, nothing in *Sprunk* indicates that one device is requesting a session key **on behalf** of another device. In fact, *Sprunk* teaches away from this feature of Claim 1 by implying that each component must individually obtain a session key **directly** from the KDC or a signaling controller.

Claim 1 features that the request from the second device to obtain the session key includes the shorter-lived symmetric key of the **first** device. *Sprunk* does not teach authenticating a request from a second device based on authenticating a shorter-lived symmetric key of a first device contained in the request from the second device, because nothing in *Sprunk* suggests that any device is sending a message with another devices symmetric key. Each CTA in *Sprunk* utilizes its own public/private key pair to communicate with the KDC. Further, each CTA in *Sprunk* communicates with a respective signaling controller using its own symmetric key.

Sprunk clearly teaches that **both** a source and destination CTA **directly** communicate with the **KDC**. Because both CTAs communicate with the KDC to receive a session key, *Sprunk* cannot teach providing a symmetric session key to the second device, wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service. In *Sprunk* both CTAs are clearly communicating with the KDC, which is a key management service. In order for each CTA to obtain a symmetric key, each CTA must communicate directly with the KDC. *Sprunk* does not teach a method where one device can receive a session key for communicating with another device without contacting a key management service.

Claim 1 features providing a session key to only the second device but *Sprunk* teaches that a key management service, or the KDC, can distribute the symmetric session keys by establishing a secure session **with each network element.** *Sprunk* at FIG. 4, for instance, shows that the Source SC (Signaling Controller) provides the CTA-to-CTA sub-key or session key to both the destination CTA and the source CTA. Thus, in order for the session key to be distributed to both devices, **both** devices must communicate with a source or destination controller, which is clearly associated with a key management service (*see* FIG. 6, where Signalling Controller 140A is connected to KDC 150A). Further, the KDC 150 distributes tickets and session keys to both CTAs 110a and 110b, so that they can use those session keys to establish secure signaling channels with signaling controllers. Therefore, *Sprunk* does not teach or suggest this feature of Claim 1.

Also, nothing in *Ganesan* or *Davis* teaches or remotely suggests one device requesting a session key on behalf of another device or providing a session key to a second device wherein a first device obtains the session key without communicating to a key management service or

authorative administrative service. Therefore, *Ganesan* or *Davis* fails to teach or suggest the method of Claim 1.

Because neither *Sprunk* nor *Ganesan* nor *Davis*, alone or in combination, teaches or suggests all of the features of Claim 1, these references cannot support an obviousness rejection of Claim 1. It is respectfully requested that the rejection of Claim 1 be reconsidered and withdrawn.

4. The Office Action Cited No Art Against Features of Claim 1.

The Office Action fails to apply any alleged prior art to a number of features of Claim 1. For example, the Office Action has failed to mention the feature that the trusted device registration service provides the first device a longer-lived symmetric key despite the fact that this feature appeared in the claim for last examination. In addition, the Office Action has failed to mention the features of receiving a message from the first device that requests network services, wherein the message from the first device contains the longer-lived symmetric key in Claim 1 despite the fact that these features in Claim 1 were presented for examination.

As a result, the Office Action has cited no art against the aforementioned features of Claim 1. It is respectfully submitted that, for this reason alone, a prima facie case of unpatentability has not been established by the Examiner with respect to Claim 1 in the rejection under 35 U.S.C. 103(a) over *Sprunk, Ganesan* and *Davis*.

For the reasons set forth above, it is respectfully submitted that Claim 1 is patentable over *Sprunk, Ganesan* and *Davis* under 35 U.S.C. 103(a).

B. Claims 2, 4, 8-10, 12-20 and 23-32

Claims 2 and 4 are dependent upon Claim 1 and thus include each and every feature of the corresponding independent claim. Therefore, it is respectfully submitted that Claims 2 and 4 are allowable for the reasons given above with respect to Claim 1.

Claim 8 contains features that are similar to those described above with respect to Claim 1. Therefore, for at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claim 8 is allowable over the art of record and is in condition for allowance.

Claims 9-10 and 13-17 are dependent upon Claim 8 and thus include each and every feature of the corresponding independent claim. Therefore, it is respectfully submitted that Claims 9-10 and 13-17 are allowable for the reasons given above with respect to Claim 8.

Claim 18 contains features that are similar to those described above with respect to Claim 1. Therefore, for at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claim 19-20 and 24-29 is allowable over the art of record and is in condition for allowance.

Claims 30-32 each recite similar features as those discussed above with respect to Claim 8. For example, Claim 30 is a computer-readable medium claim that corresponds to method Claim 8. Claim 31 is recited in a format allowable by 35 USC §112, and corresponds to method Claim 8 discussed above. Claim 32 is an apparatus claim that corresponds to method Claim 8. Therefore, Applicants respectfully submit that Claims 30-32 are patentable for at least the same reasons discussed above as to Claim 8.

IV. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: July 10, 2006

Zhichong Gu
Reg. No. 56,543

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080 x236
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on July 10, 2006 by Martina Placid
Martina Placid